DS for EM

Distributed Systems for Energy Management

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Peter Palensky
University of Pretoria

Feb 19, 2009

Who/where am I?

- Previously: Vienna Univ. of Technology, AUSTRIA

- Envidatec Corp., Hamburg, GERMANY
  - Energy (data) management
- University of Pretoria, SOUTH AFRICA
  - Professor for embedded systems, information security
- Hanyang University, Seoul, KOREA (2009)
  - Guest Prof.: Building automation, computer networks

3 research areas

- Networked Embedded Systems
  - Building automation
  - Communication protocols
  - Dependable Systems
- Energy Automation
  - Load Management, Remote Metering and Sensing
- Cognitive Science
 - Psycho-biomimetics for automation systems

Topic: the future Energy System

- Lots of new things in the "**smart grid**"
  - Distributed generation, responsive loads,
  - On-line information and metering, energy storage, real-time price signals,
  - bi-directional & automated distribution,…
- Support by <u>distributed (IT) systems</u>
  - Servers, sensors, control modules, data loggers,…
  - Communication links, algorithms, rules,…
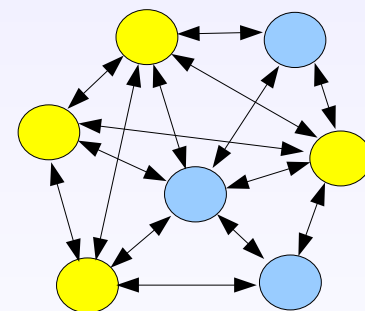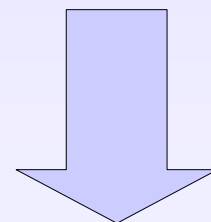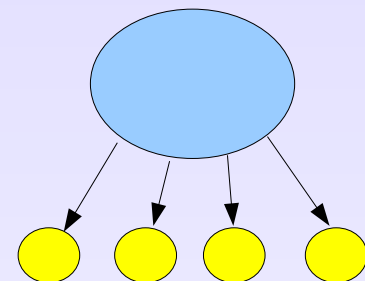
DOE: "silver buckshot"

Today's subject

Discuss parts, problems and methods of distributed systems for energy management

A.) Energy information systems

B.) Load management

C.) Machine-to-Machine communication

- M2M Information security
- Embedded systems reliability

D.) Simulation of distributed automation
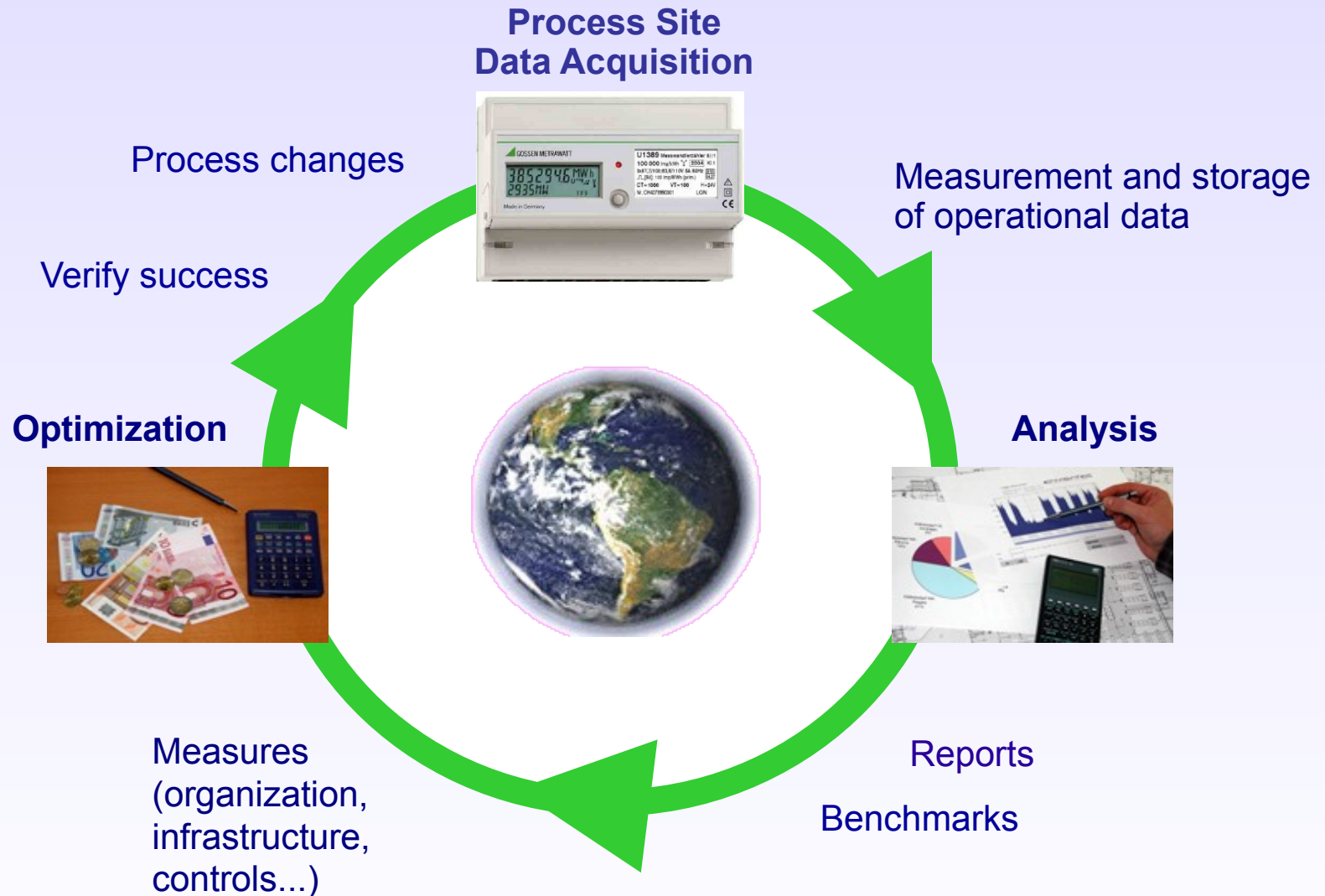
E.) Future research

Involved sciences for DS for EM

- Computer Engineering
  - Embedded systems, telecommunication
- Computer Science
  - Distributed algorithms, software methodologies
- Electrical / Power Engineering
  - Energy distribution, control engineering
- Modeling, Simulation
  - Distributed state machines, physical processes
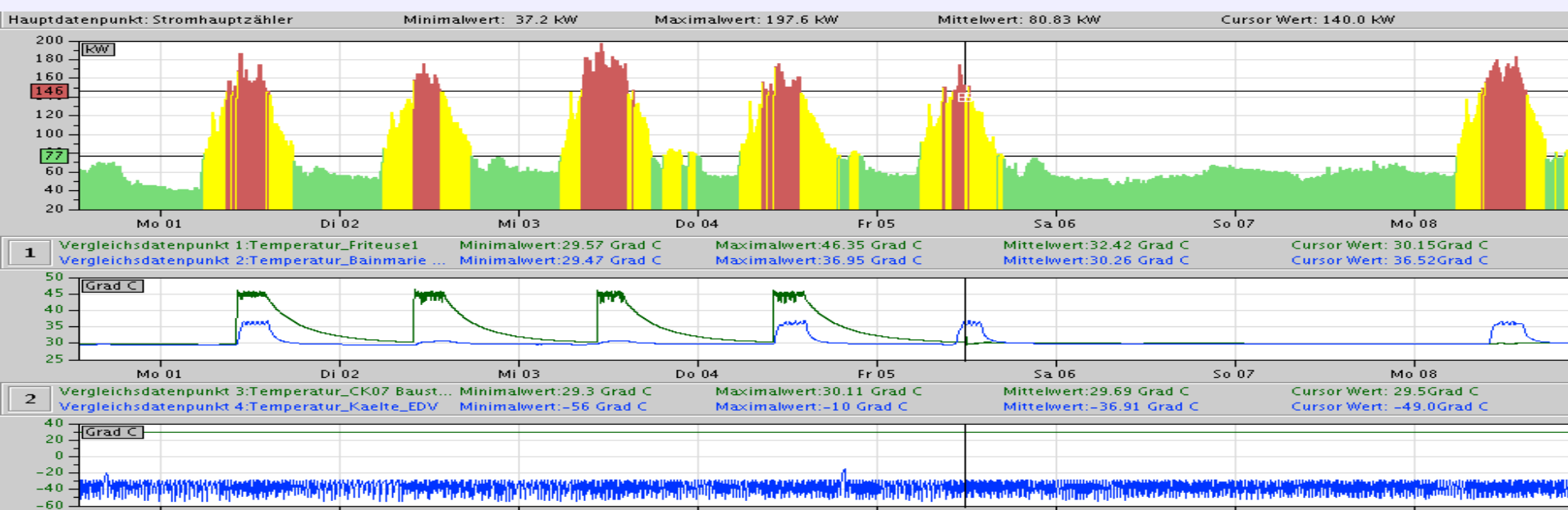
plus systems thinking

A.) Energy Information Systems

Process Site Data Acquisition

Measurement and storage of operational data

Analysis

Reports

Benchmarks

Measures (organization, infrastructure, controls...)

Optimization

Verify success
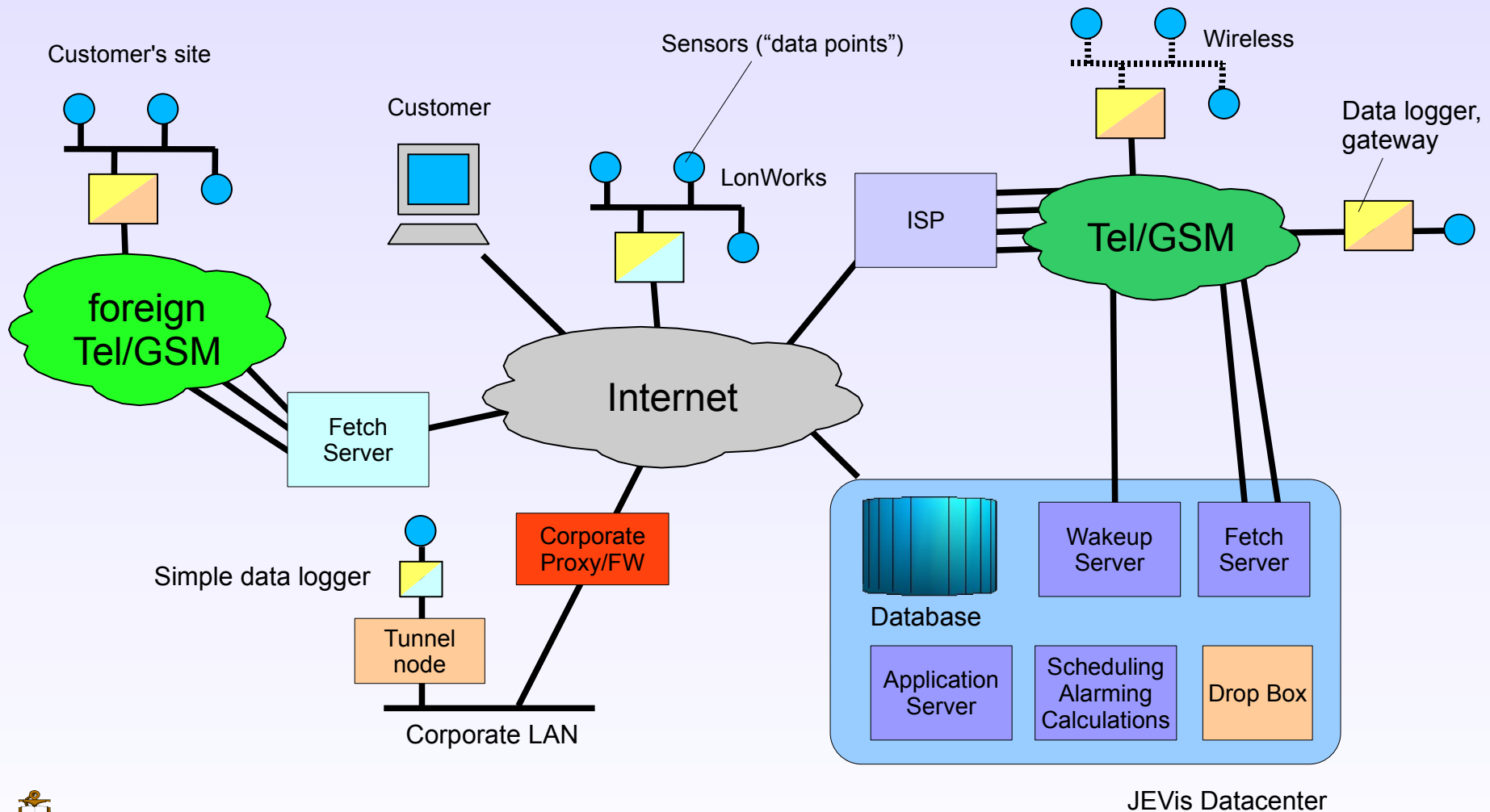
Process changes

Measurement data time series analysis

- Energy, temperature, machine operation,...
- My-JEVis.com System (commercialized research project)
  - Server-side analysis (Java, Matlab/Octave and R)
  - Correlations, frequency analysis, trends,...
  - Benchmarking of multi-site customers

Simplified system architecture

Customer's site

Sensors ("data points")

Wireless

Customer

LonWorks

Data logger, gateway

ISP

Tel/GSM

foreign Tel/GSM

Internet

Fetch Server

Simple data logger

Corporate Proxy/FW

Tunnel node

Corporate LAN

Database

Wakeup Server

Fetch Server

Application Server

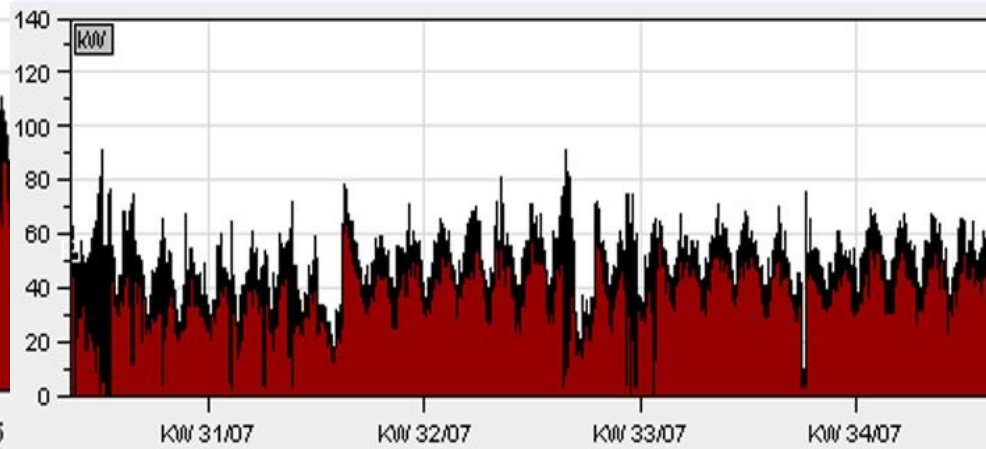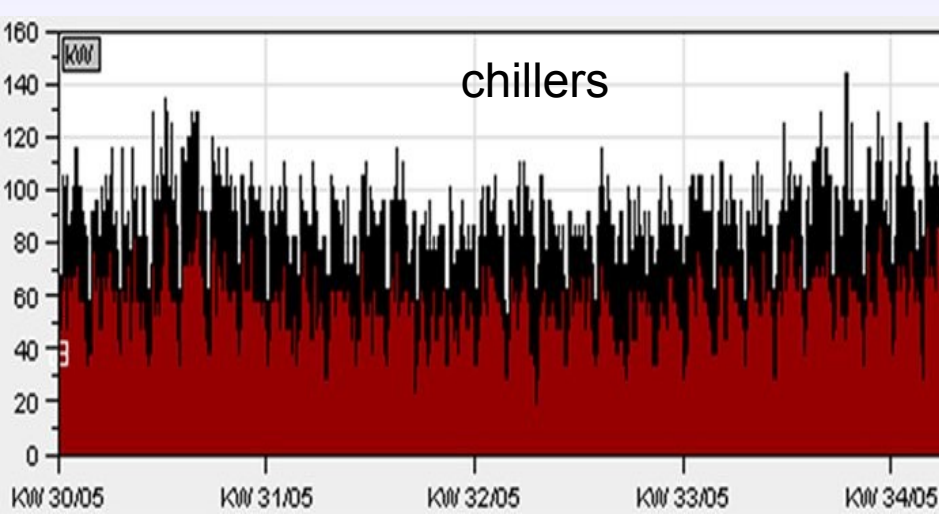Scheduling Alarming Calculations

Drop Box

JEVis Datacenter

Devil in details: data quality, watchdogs,...

Example: Lufthansa SkyChefs

- 7 Mio. bottles wine, 1700t veg., 400t poultry,...
  - Energy costs: 305 kEUR
  - Long-term analysis (3 years), hundreds of "data points"
- Optimized controls, use of waste heat, new equipment
 - -56 % Electricity, -72 % Heating, -59 % CO_2

chillers

My-Jevis.com: next steps

- Automatic analysis
  - Formalize expert knowledge
  - Integrate process simulations
    - Energy+, HW-in-the-loop simulation, model refinement
- Universal database
  - The "SAP for environmental/physical data"
  - Open source
- Integration with Load Management Systems
  - Back to the roots...
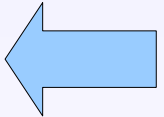
B.) Load Management System

- Traditional architecture
- Shed limitations
  - Max twice daily,
    max 30min,
    not 8am-10am,...
- Desired load profile
  - P_{max}, schedule,...
- 1 Energy meter
- Priorities

consumers

rules

E-Ctr | Central
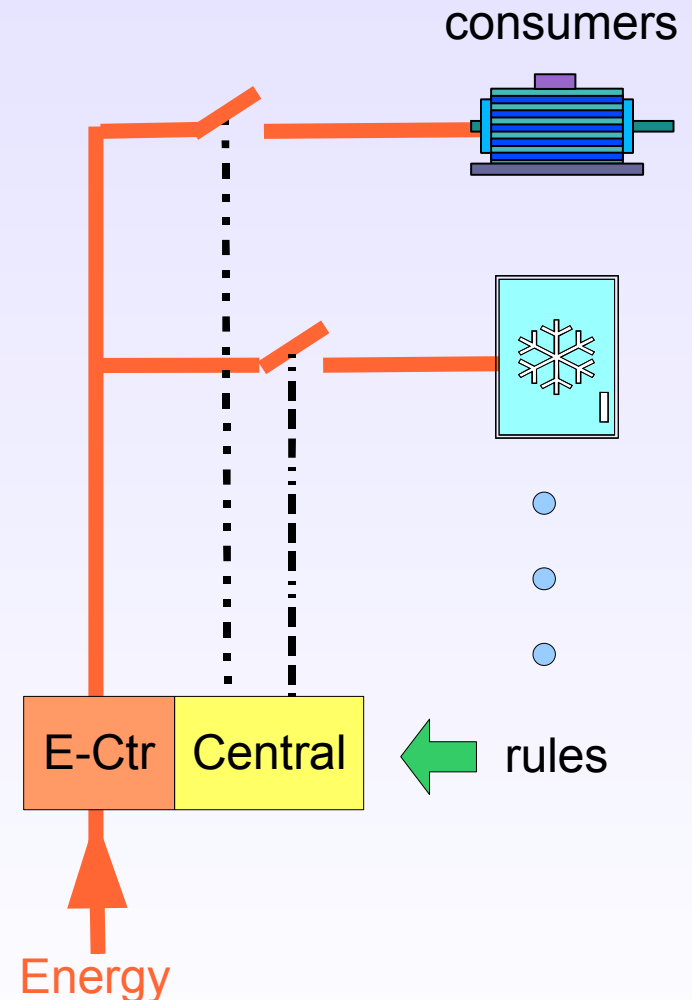
Energy

- Energy trajectory

- Static priorities
  - P1>P2>P3

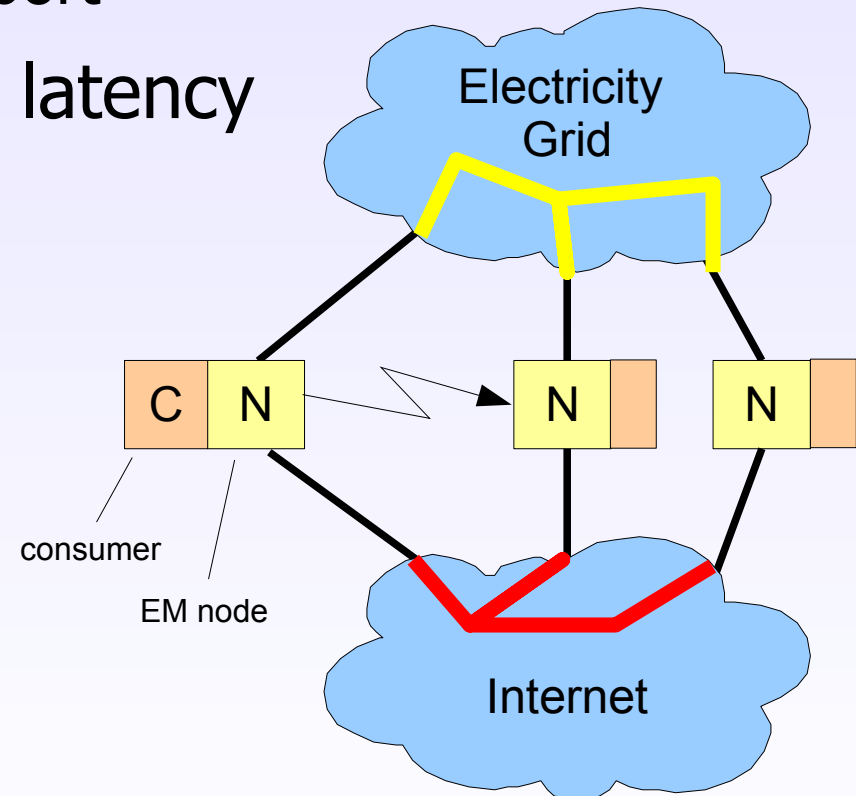- New potential goal every t_p (15min)

Better load management

- Limitation of centralized design
  - No process model, no planning
- Smart Fridge
  - Embedded EM node
    - Software agent, power electronics,...
  - Coordinated control
- IRON box
  - Wireless communication
  - Low cost
  - Learns process
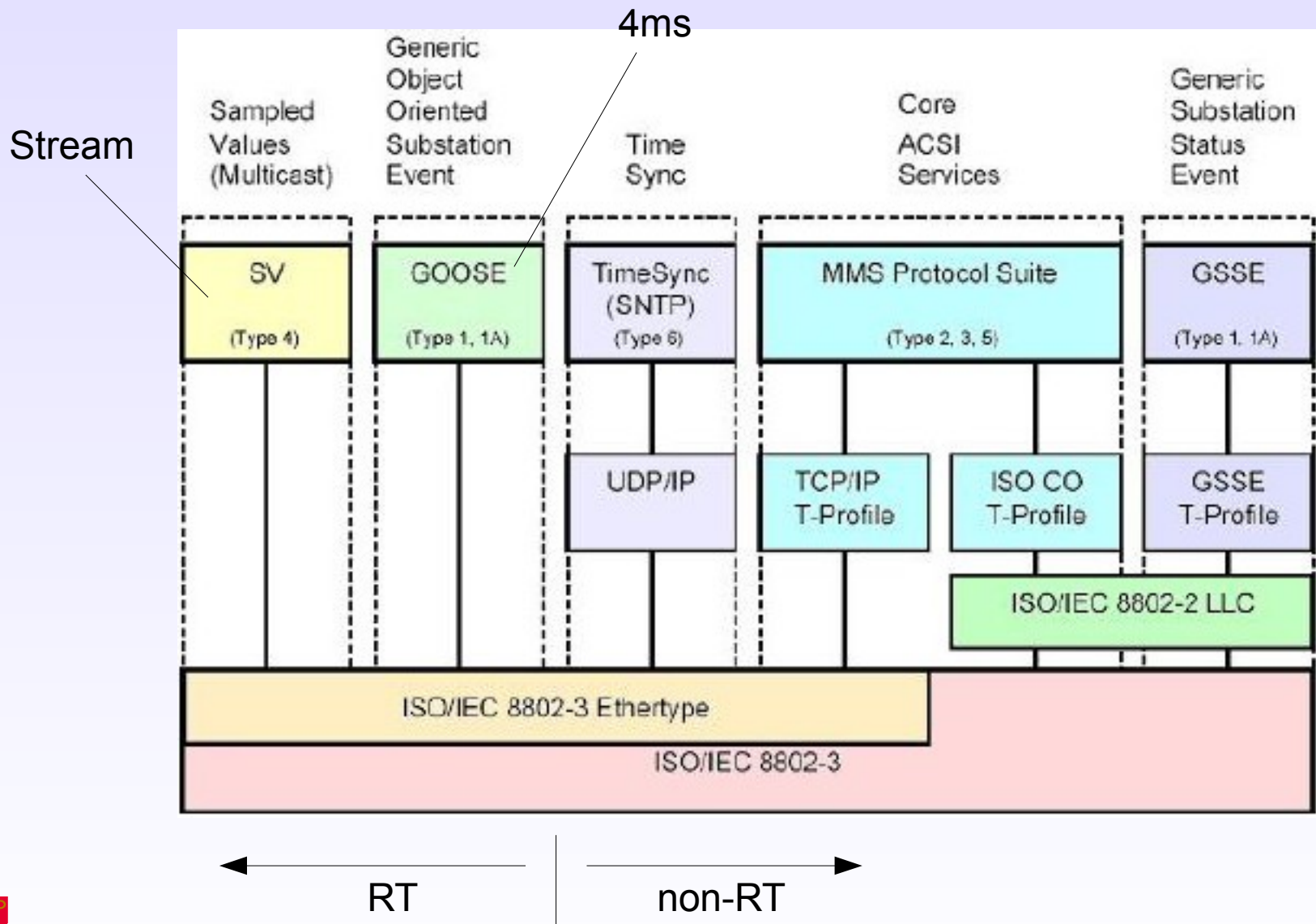
Peter Palensky   Feb 19, 2009   DS
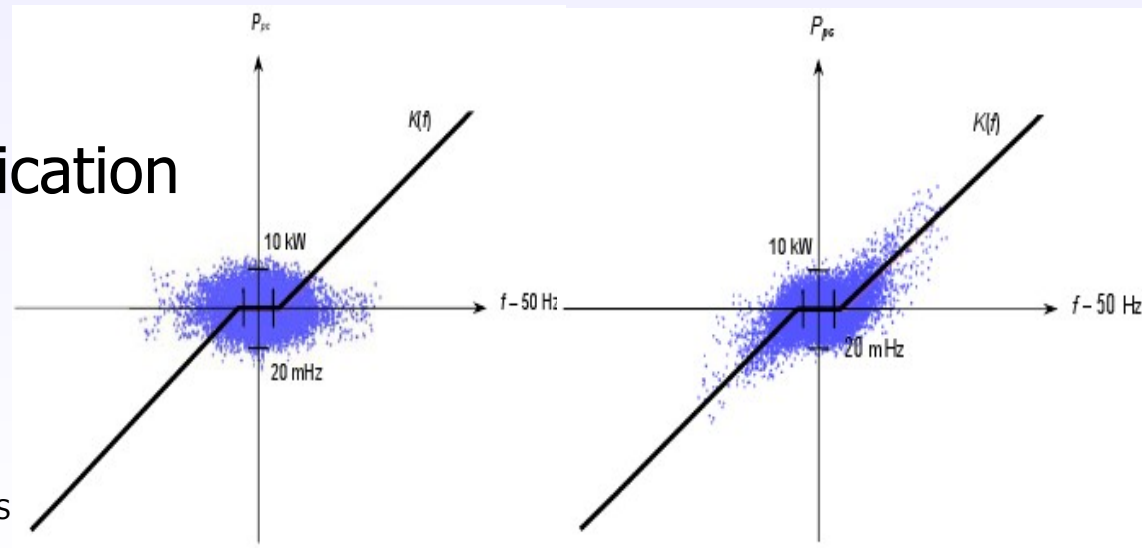
Wide Area Load Management

- Just do it over the Internet?
  - Network based control over *best effort* transport?
  - NBC needs real time transport
- E.g.: satellite link: 250ms latency
- RT/leased line: $$$
  (real-time)
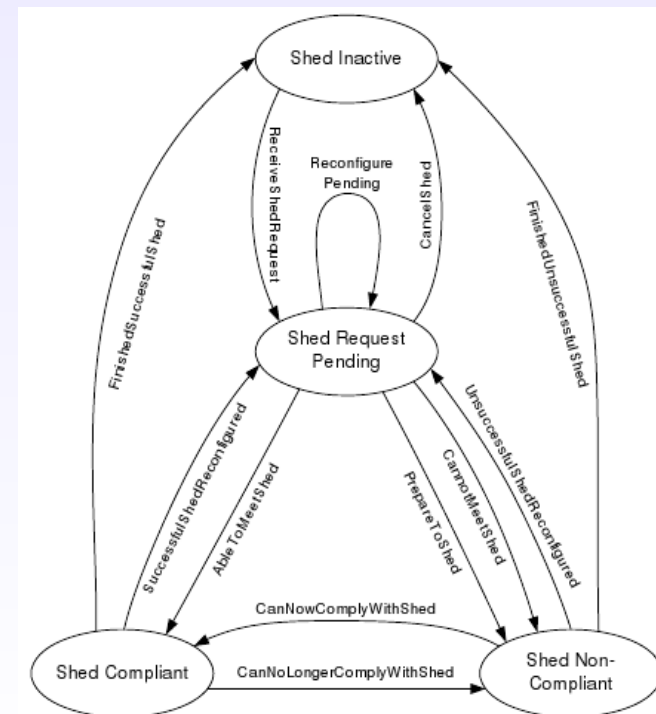- New: "hybrid" networks
  - Grid frequency
  - Leased-line on demand

Electricity Grid

C N   N   N

consumer

EM node

Internet

Compare IEC 61850
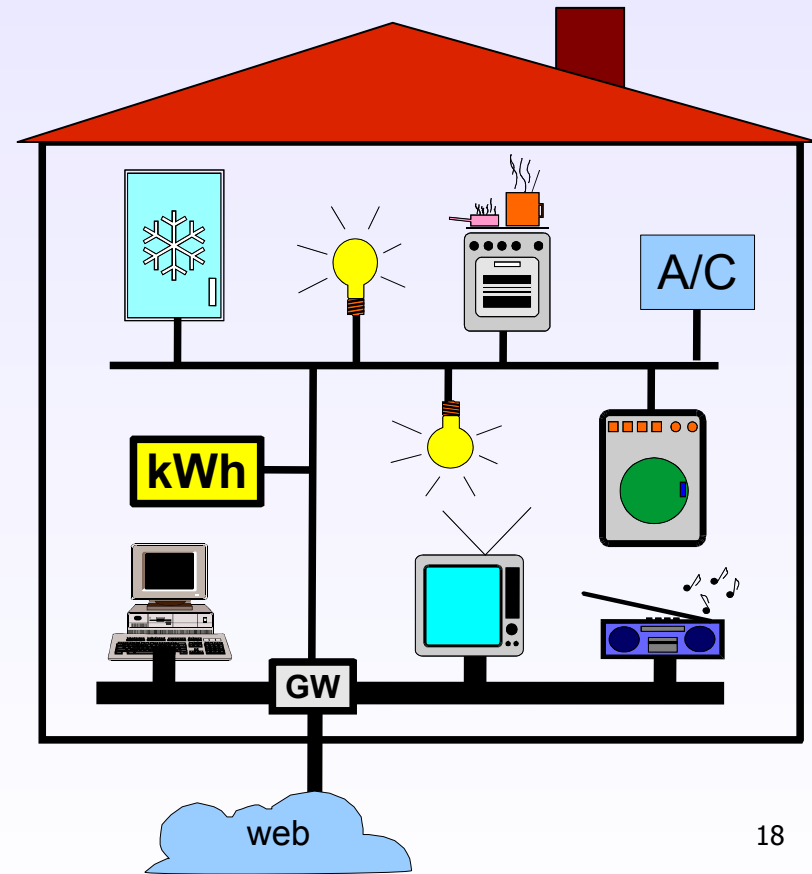
Goal: EM interface/algorithm

- ● Physical Interface: any

- ● Logical Interface / Profile

  - ● Zigbee Smart Energy Profile (200+ pages)
    - • Shedding, metering, time-of-use prices, display, PCT...

  (PCT: Programmable Communicating Thermostat)

  - ● IEC 61850 Standard (huge)
    - • Data types, transport

  - ● BACnet Load Control Object (18 pages)
    - • Shed duration, shed level (%),...

  - ● Working with LonMark, OASIS

C.) Machine-to-machine communication

- Scenario: Building2grid & IT-Security
  - Remote control/diagnosis, energy prepayment, DR,...

    (Demand Response)
- End-to-end security
  - **C**onfidentiality (encryption)
  - **I**ntegrity (checksums)
  - **A**uthenticity (e-signatures)
  - M2M Trust / Identity
    - PIN / TAN? (Personal Identification / TransAction Number)
    - Key distribution
- Standards ←

A/C

kWh

GW

web

Building Networks & IT Security 1

- LonWorks

  - Integrity and Authentication (Layer 5)

  - Proprietary, symmetric 48 Bit method

  - Challenge-Response with 64 Bit nounce

  - Key distribution not secure

  - Only one key per node

  - Network management messages not protected

    - ReadMem!

  - Good: Authentication

  - Bad: Rest

Building Networks & IT Security 2

- KNX

  - Password-based access control
  - 4-Byte plain-text password per access level (255)
    - Application parameters, program,
    - Address tables, etc.
  - Memory protection
  - No Authentication or encryption
  - No protection from „Replay-Attacks"
  - Good: Access Control
  - Bad: Rest

Building Networks & IT Security 3

- BACnet
  - Central key-server (client, server)
  - Symmetric 56 Bit DES encryption (DES: Data Encryption Standard)
  - Authentication via challenge-response
  - Session Keys distributed by key-server
  - Operator authentication: user name
  - Protection against Replay Attacks
  - Good: a lot
  - Bad: old methods, central server, same key for encr. & auth.

Add better cryptography?

- In Software?
  - Keys not protected (Kerkhoff!)
  - Low-performance hardware

- Secure micro chips
  - Smart Card
    - Gemalto Cyberflex $30: AES, RSA, SHA-1, etc.
  - Trusted Platform Module TPM
    - Infineon SLD9630 $10: SHA-1, RSA
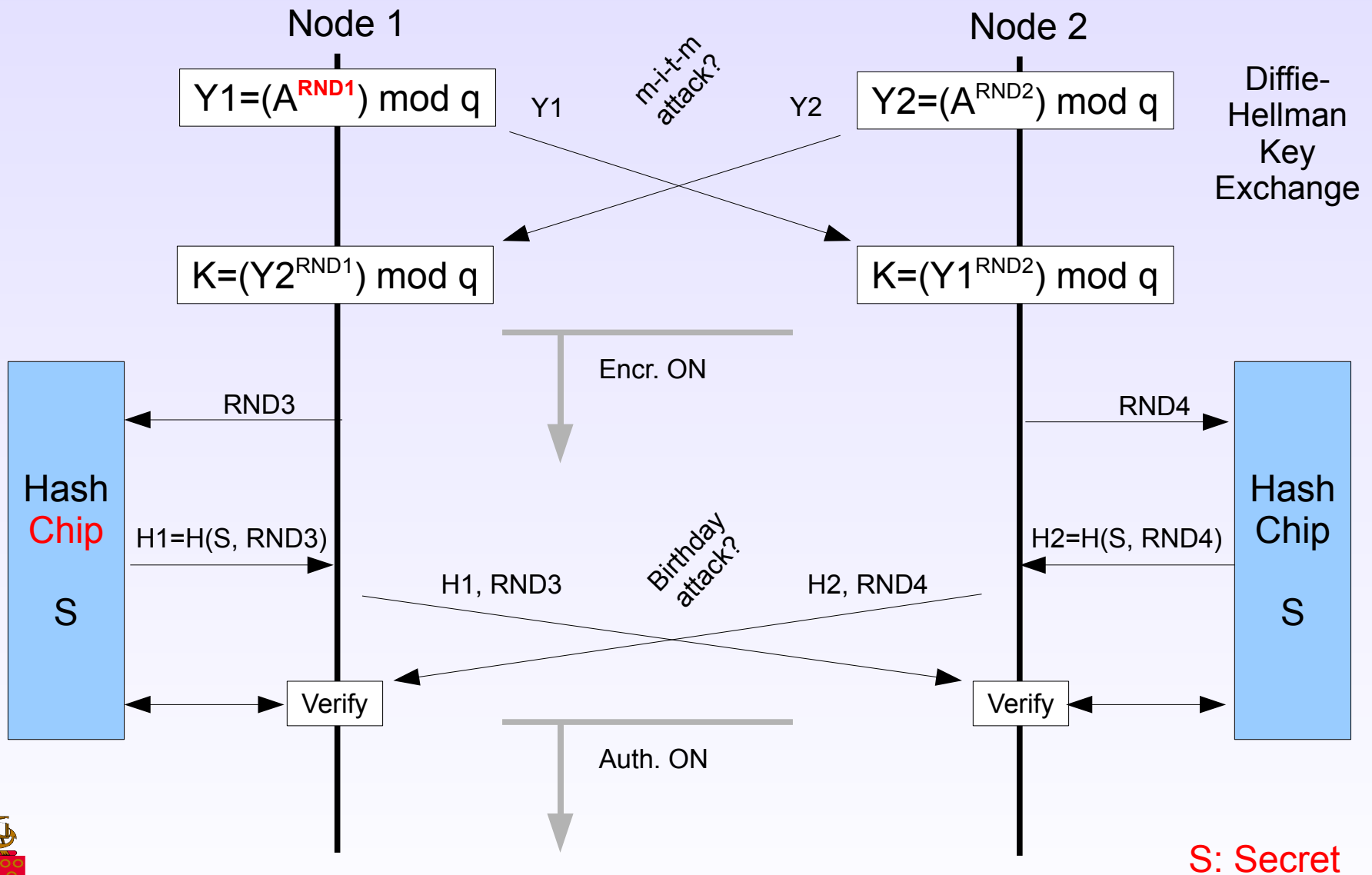 - Low-cost Hash Chips
    - Dallas DS28E01 $0.5: SHA-1

Challenge → | **Crypto HASH Function**

H(Challenge, Secret) ← | **Secret**

Low-cost m2m Security

Node 1

Node 2

m-i-t-m attack?

$Y1=(A^{RND1})$ mod q

$Y1$

$Y2$

$Y2=(A^{RND2})$ mod q

Diffie-Hellman Key Exchange

$K=(Y2^{RND1})$ mod q

$K=(Y1^{RND2})$ mod q

Encr. ON

RND3

RND4

Hash Chip S

Hash Chip S

$H1=H(S, RND3)$

$H2=H(S, RND4)$
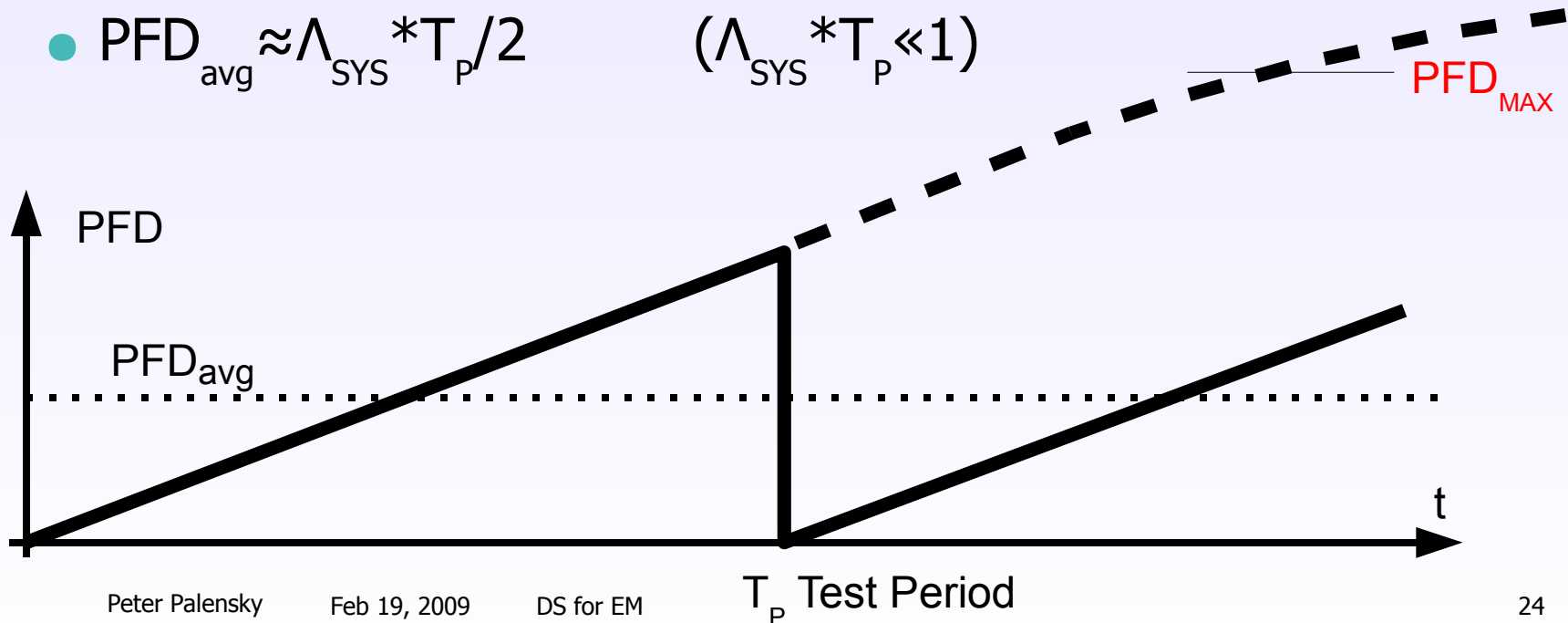
H1, RND3

Birthday attack?

H2, RND4

Verify

Verify

Auth. ON

S: Secret

Inf. security → reliability?

- E.g. Safety Integrity Levels SIL 1-4 (IEC 61508)
- PFD: Probability Failure on Demand
  - SIL3: $PFD_{avg} < 10^{-3}$
  - $PFD = 1-e^{-(\Lambda sys*t)}$ (Λ = failure rate)
  - $PFD_{avg} \approx \Lambda_{SYS}*T_P/2$ ($\Lambda_{SYS}*T_P \ll 1$)

PFD_{MAX}

PFD

PFD_{avg}

T_P Test Period

t

Additional help: redundancy

- M-out-of-N architecture: $\Lambda_i = \Lambda$, binomial distr.

$$\Lambda_{SYS} = \sum_{k=n-m+1}^{n} \frac{n!}{k!(n-k)!} \Lambda^k (1-\Lambda)^{(n-k)}$$

3oo5:

5F
4F
3F
2F
1F
0F

- 1oo1: $\Lambda_{SYS} = \Lambda$
- 1oo2: $\Lambda_{SYS} = \Lambda^2$
- 1oo2D: $\Lambda_{SYS} = (\Lambda*(1-DC))^2$ (Diagnostic Coverage)

(mutual) **D**iagnosis

- $PFD_{avg\_1oo2D} = (\Lambda*(1-DC))^2 * T_P^2/3 + ...$

(e.g. Test for 60%-90% DC of 64kB memory:10h!)

- Distributed Resource Management
- Goal:
  - Investigate algorithm and (hybrid) communication
  - Scalability, <u>robustness</u>, performance
  - HW resource needs
- Not the goal:
  - Accurate local process simulation
  - Hi-Res load flow analysis (DigSilent, Neplan)
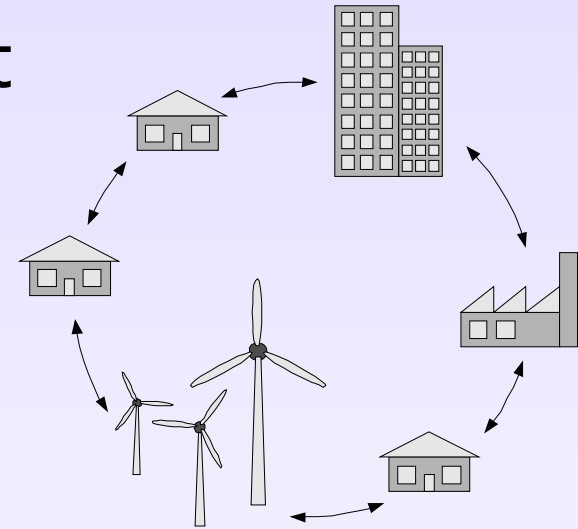
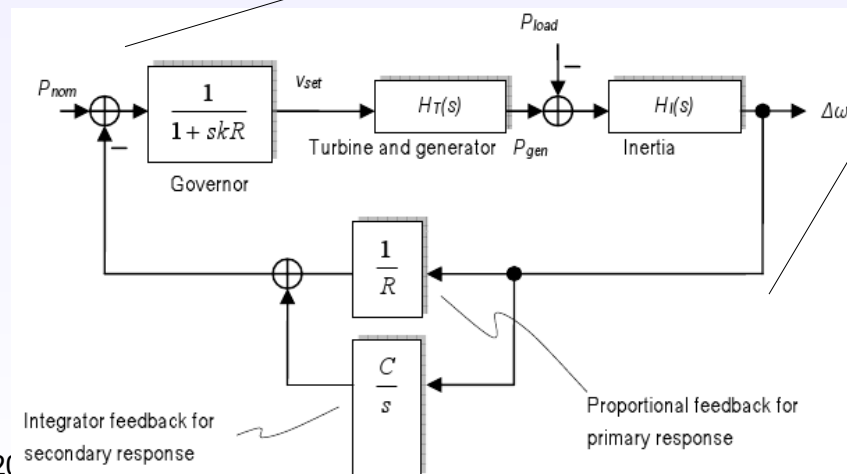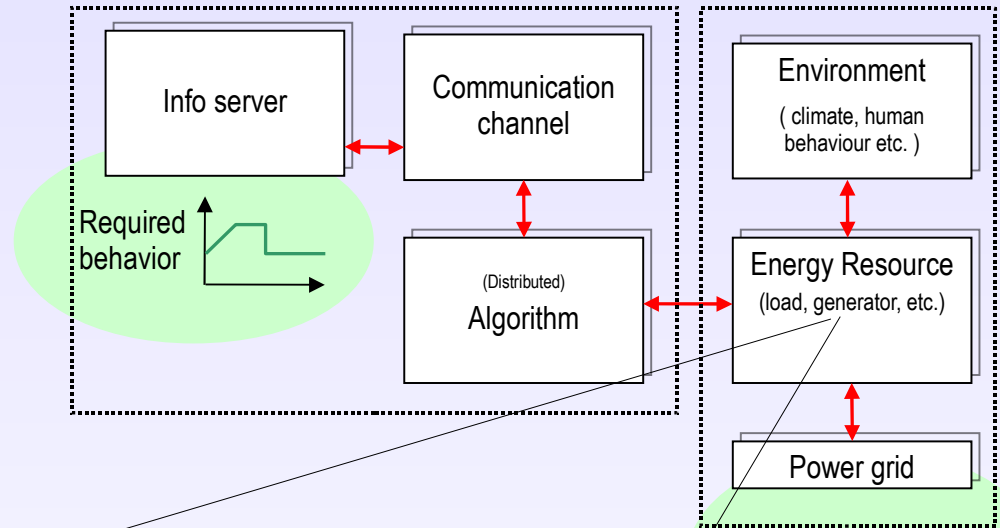# Simulation Platform

- Power system simulation
  - Matlab prototypes
  - Translate to OMNeT++
    - Telecommunications
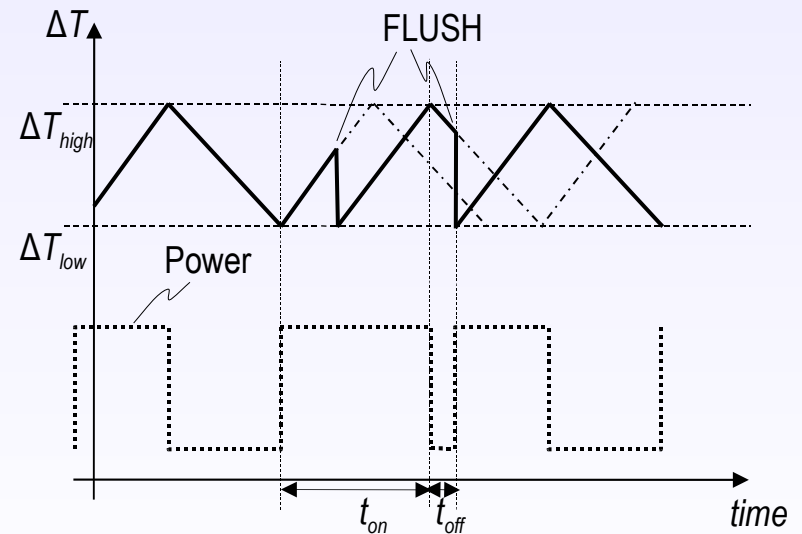   - Discrete event simulator open source, cross-platform
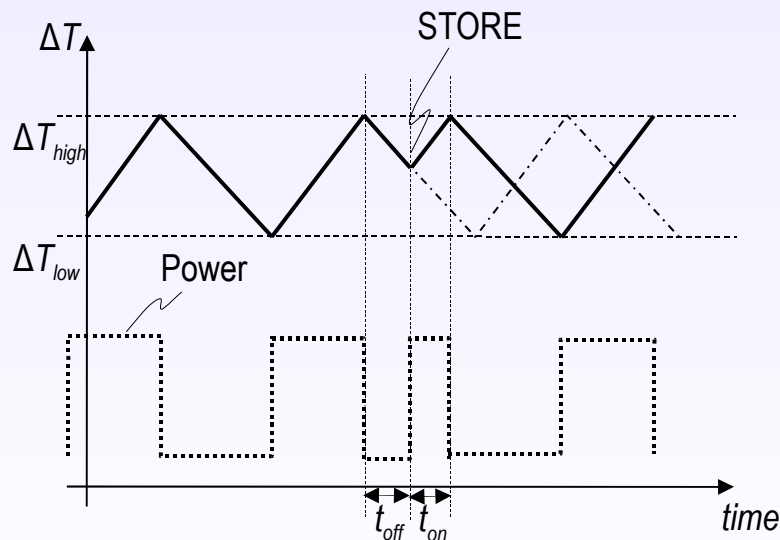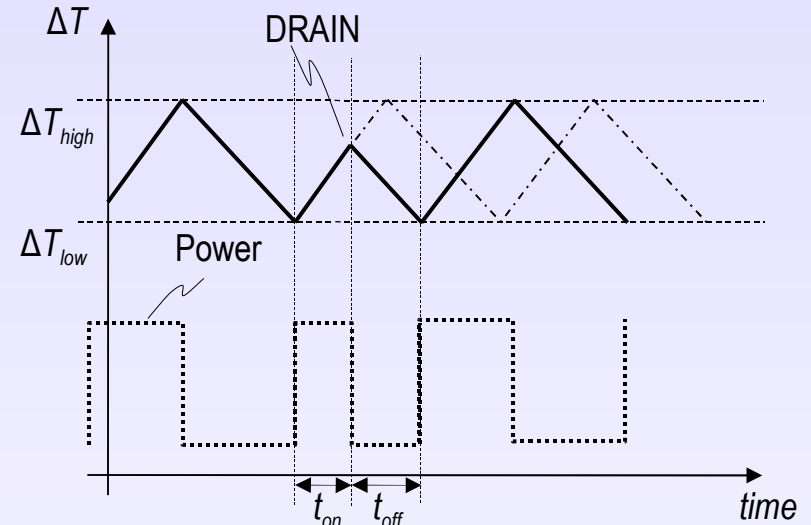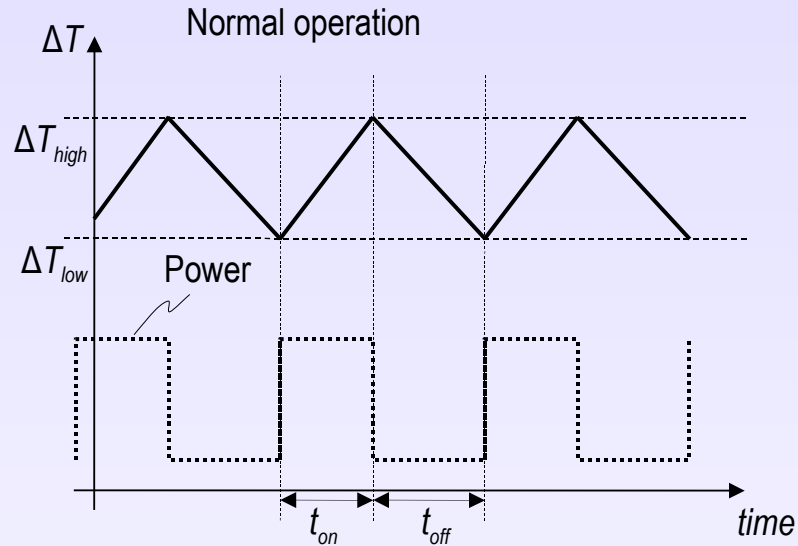- Models of
  - Generators, loads, grid,...
- Testing
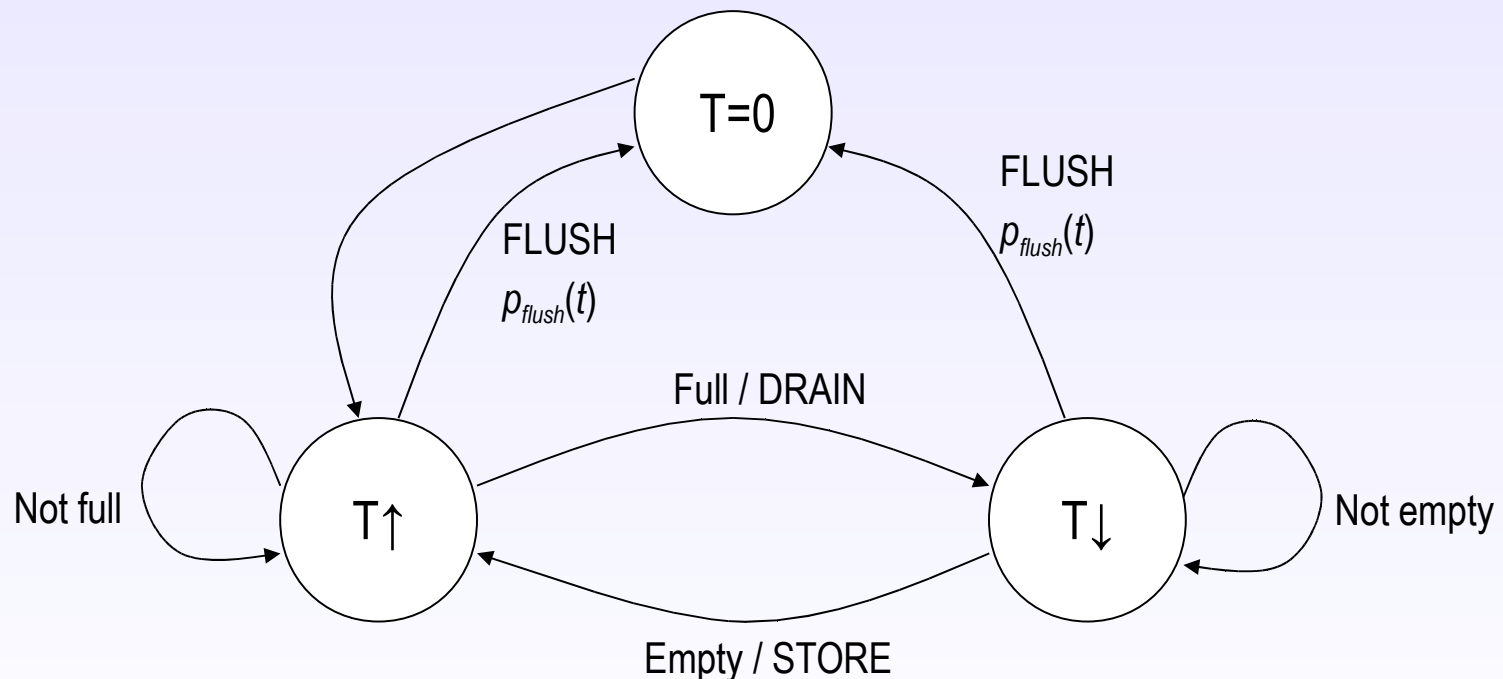 - Algorithms
  - Communication

Example: Model for HVAC

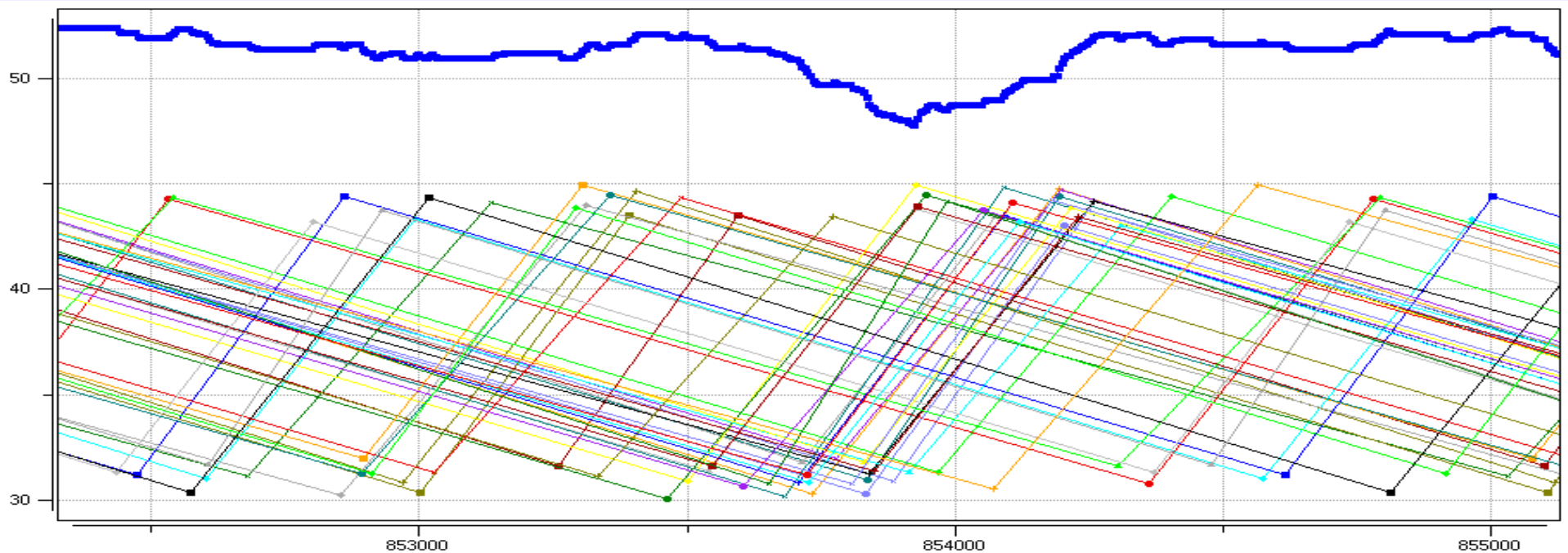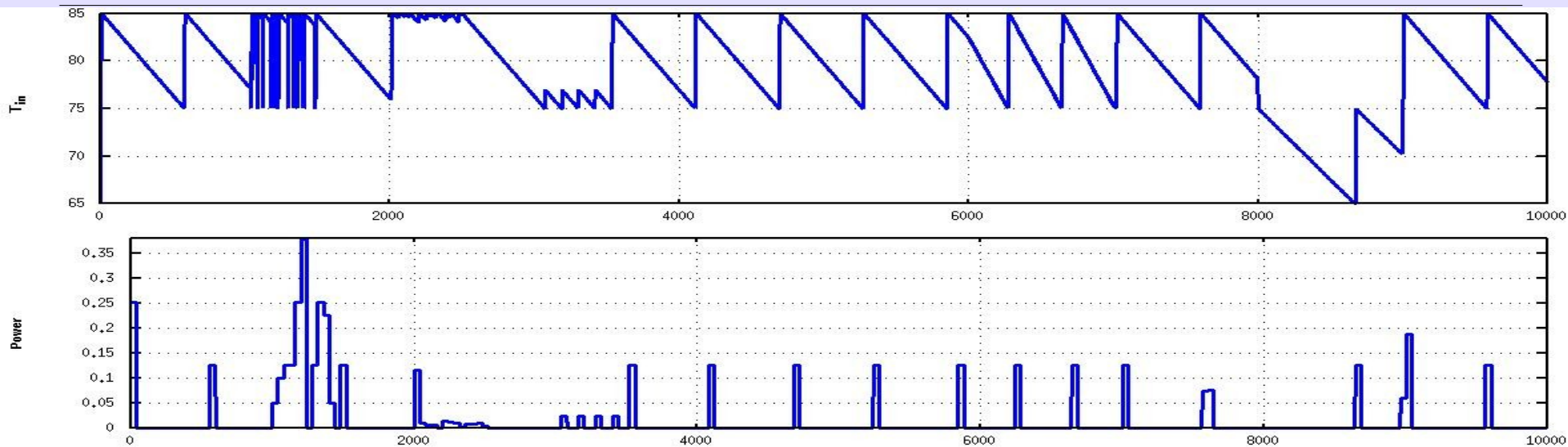(Heating Ventilation and Air Conditioning)

Example: Model for HVAC (cont'd.)

- Initially: continuous model, 28 state discrete, etc.
- → (Extremely) simplified Markov model with three states
- Internal variable: virtual energy storage T (thermal inertia)

Implementation of simple HVAC model

Results, next steps

- Simplified Markov models and "events"
  - For every resource type
    - Lighting, pumps, distributed generation, batteries,...
  - As simple EM language

- To do
  - Very simple algorithms
  - Tests: grid/com failure/overload, ...
  - Performance, stability limits, scalability
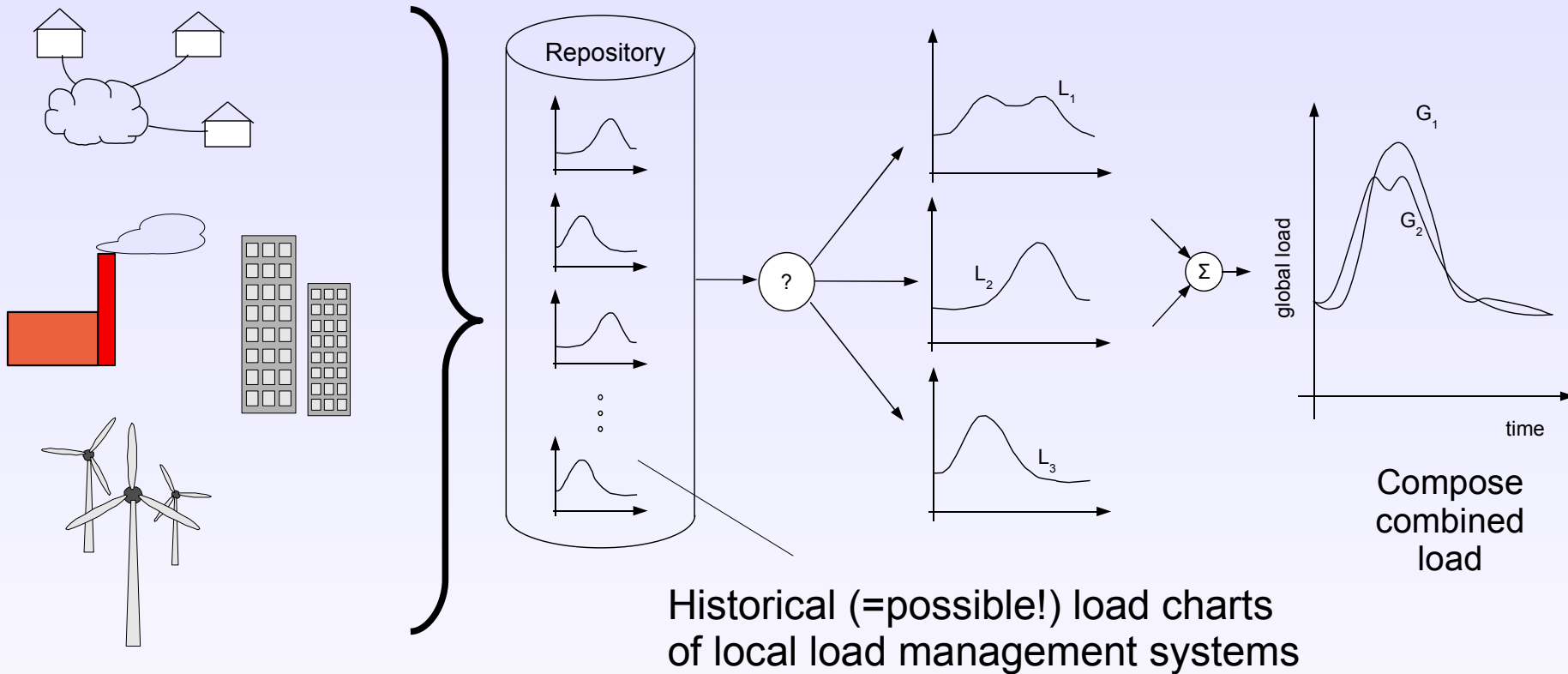 - Mutual diagnostics within system (1oo1D, 1oo2D)

E.) Future research

- New Project

- Virtual power plant + virtual pump storage(!)

- Integration of
    - Energy information system
    - Distributed load management
    - Reliable infrastructure
    - Smart distribution automation

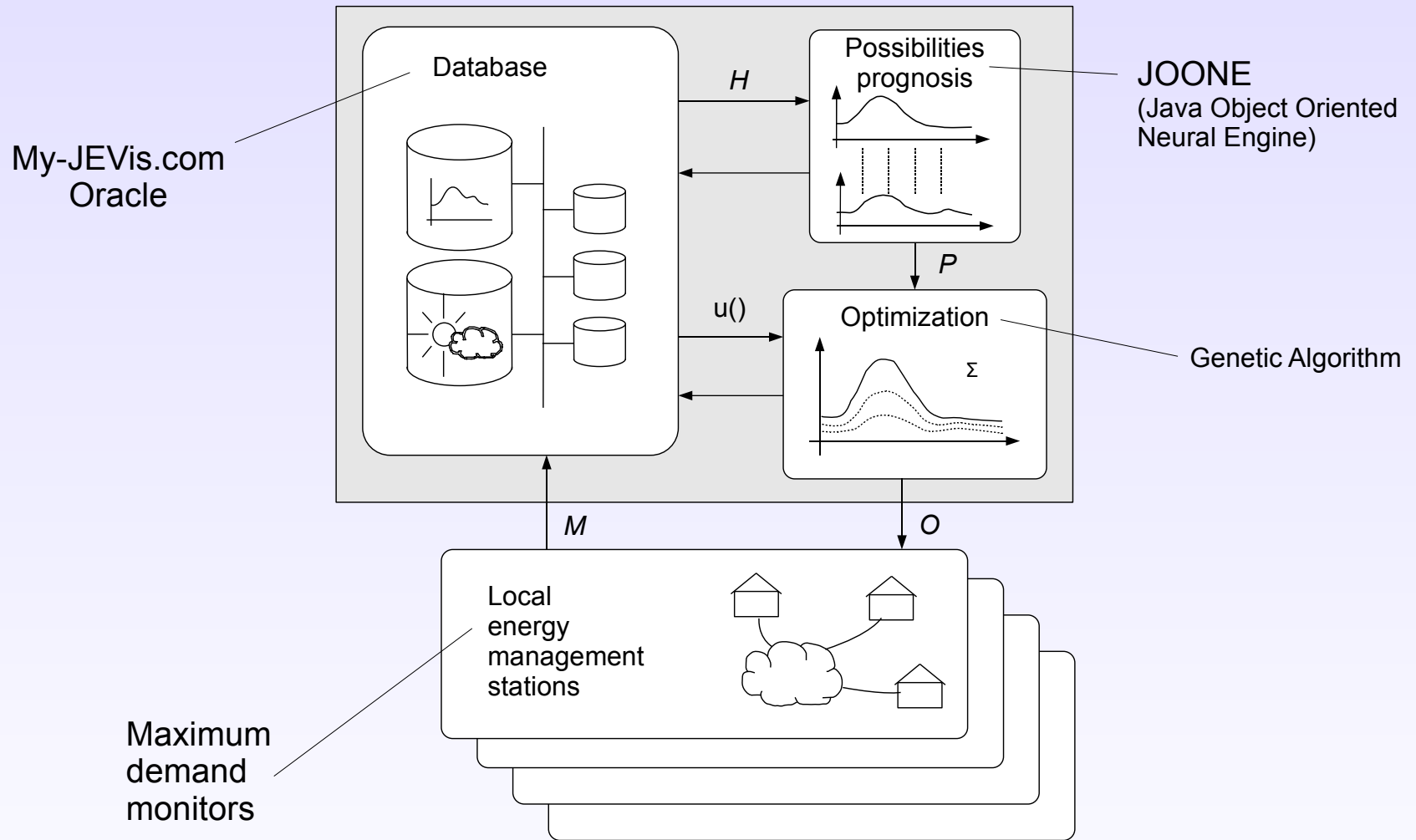# First step: EIS + load management

Participants equipped with (and without) local energy management

Repository

Historical (=possible!) load charts of local load management systems

L_1

L_2

L_3

G_1

G_2

global load

time

Compose combined load

First step: EIS + load management

My-JEVis.com
Oracle

Database

H

Possibilities prognosis

JOONE
(Java Object Oriented
Neural Engine)

u()

P

Optimization

Σ

Genetic Algorithm

M

O

Local
energy
management
stations

Maximum
demand
monitors

Challenge: reduce/select infinite possibilities to finite search space

The goal

Integrated, distributed IT infrastructure for wide area energy management

- Simple EM interface language
  - Use Markov models
  - Interoperability, OASIS profiles
- Dependable architecture
  - Self-organizing and -healing → simulation
- Boxes → open core silicon
  - Compare "green plug"?

Conclusion

- Path to "smart grid" not easy
  - Interdisciplinary, breadth and depth…
  - Simulation, verification
- Challenges solvable
  - Load models, dependability, communication,…
- White spots
  - Scalability, stability,…

Q&A

- Energy information systems

- Load management

- Dependable m2m communication

- Simulation of distributed algorithms